

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 214 Centenary Church Road  
 Clemmons, North Carolina 27012-7301

Case No. 1:22MJ421-1 JW  
 1:22MJ421-1

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Middle District of North Carolina  
 (identify the person or describe the property to be searched and give its location):

Please see Attachment A attached hereto and incorporated herein

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B attached hereto and incorporated herein

YOU ARE COMMANDED to execute this warrant on or before November 4, 2022 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Joe L. Webster

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for      days (not to exceed 30) ☐ until, the facts justifying, the later specific date of     

Date and time issued: 10/21/2022 7:43 am

  
 Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge  
 Printed name and title

**Return**

Case No.:

~~1:21MJ421-1~~ 1:22MJ421-1

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## ATTACHMENT A

### *Property to be searched*

The property to be searched is 214 Centenary Church Road Clemmons, North Carolina, 27012-7301: a free-standing single-family home with light brick, tan siding, a gray roof, and an attached garage with white garage doors.



## ATTACHMENT B

### *Property to be seized*

1. All information and records, that constitute evidence, instrumentalities, contraband, and fruits of a violation of Title 18, United States Code, Sections 1030(a)(2) (intentionally accessing a computer without authorization), 1030(a)(4) (accessing a computer without authorization with the intent to defraud), and Title 18, United States Code Section 371 (conspiracy) involving Christopher Clampitt and unauthorized access to social media accounts or other image storage (i.e. cloud storage, etc.) occurring over an unknown timeline, including:

- a. Records and information relating to the unauthorized accessing of phones, social media platforms, file hosting/sharing sites, and other media maintained by victims on private computers or accounts;
- b. Records and information relating to practices, strategies, tools, or products to facilitate unauthorized access to protected accounts and/or devices;
- c. Records and information related to the purchase or trials of software for automated SMS and/or calls;
- d. Records and information concerning the downloading and storage of private images and materials belonging to victims, as well as means to share images with others;
- e. Records related to targeting victims, such as identifying information, phone numbers, social media handles, etc.;
- f. Records and information concerning sites, forums, or groups for sharing illicitly obtained personal images;

- g. Records and information regarding any sharing, selling, or posting of illicitly obtained images;
    - h. Images and videos of victims obtained as a result of unauthorized access to the victims' social media accounts;
  - 2. Any and all computers, phones, digital storage devices, and network equipment used as a means to commit the violations identified above.
  - 3. For any computer, phone, or digital storage devices whose seizure is otherwise authorized by this warrant, and any computer, phone or digital storage devices that contain or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of access, use, and events relating to the crimes under investigation and to the COMPUTER user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crimes under investigation;
- f. evidence of the attachment to the COMPUTER;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “COMPUTER” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, SD cards and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.